COOLEY LLP
MICHAEL G. RHODES (116127)
(rhodesmg@cooley.com)
WHITTY SOMVICHIAN (194463)
(wsomvichian@cooley.com)
COLIN S. SCOTT (318555)
(cscott@cooley.com)
101 California Street, 5th Floor
San Francisco, CA 94111-5800
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

PRIYAMVADA ARORA (301207)
(parora@cooley.com)
3175 Hanover Street
Palo Alto, CA 94304-1130
Telephone: (650) 843-5000
Facsimile: (650) 849-7400

Attorneys for Defendant
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

FRANK D. RUSSO, KOONAN LITIGATION CONSULTING, LLC and SUMNER M. DAVENPORT & ASSOCIATES, LLC, on behalf of a similarly situated class,

Plaintiffs,

v.

MICROSOFT CORPORATION,

Defendant.

Case No. 4:20-cv-04818-YGR

CLASS ACTION

DEFENDANT MICROSOFT CORPORATION'S MOTION TO DISMISS PLAINTIFFS' COMPLAINT

Date: December 1, 2020
Time: 2:00 p.m.
Hon. Yvonne Gonzalez Rogers

TABLE OF CONTENTS

Page

NOTICE OF MOTION AND MOTION TO DISMISS 1
MEMORANDUM OF POINTS AND AUTHORITIES 1
I. INTRODUCTION 1
II. BACKGROUND 3
A. MICROSOFT 365 SERVICES. 3
B. PLAINTIFFS. 3
C. PLAINTIFFS' ALLEGATIONS. 4
D. THE ALLEGED CAUSES OF ACTION & PROPOSED CLASS. 6
III. ARGUMENT 6
A. PLAINTIFFS FAIL TO ALLEGE FACTS PLAUSIBLY SHOWING THEY WERE AFFECTED BY ANY OF THE ALLEGED CONDUCT. 6
B. THE WTA, SCA, AND WPA CLAIMS FAIL BECAUSE PLAINTIFFS DO NOT ALLEGE THAT THE ALLEGED PRACTICES INVOLVED THEIR COMMUNICATIONS. 9
C. PLAINTIFFS' WTA CLAIM FAILS FOR ADDITIONAL REASONS. 10
1. PLAINTIFFS DO NOT ALLEGE MICROSOFT INTERCEPTED ANY COMMUNICATIONS IN "TRANSMISSION." 10
2. THE "ORDINARY COURSE OF ITS BUSINESS" ("OCB") EXCEPTION BARS PLAINTIFFS' CLAIM. 12
D. PLAINTIFFS' SCA CLAIM FAILS FOR ADDITIONAL REASONS. 14
1. THE "NECESSARILY INCIDENT" EXCEPTION BARS PLAINTIFFS' CLAIM. 14
2. THE SCA CLAIM DOES NOT APPLY TO MICROSOFT'S OWN USE OF DATA. 15
E. THE WASHINGTON PRIVACY ACT CLAIM FAILS FOR MULTIPLE ADDITIONAL REASONS. 16
F. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE WASHINGTON CONSUMER PROTECTION ACT. 17
1. THE CPA CLAIM IS SUBJECT TO RULE 9(B)'S HEIGHTENED PLEADING STANDARD. 18
2. PLAINTIFFS FAIL TO ALLEGE MICROSOFT'S PURPORTED MISCONDUCT CAUSED THEIR INJURIES. 19
3. PLAINTIFFS DO NOT ADEQUATELY ALLEGE CPA INJURY 21
G. PLAINTIFFS FAIL TO STATE A CLAIM FOR INTRUSION UPON SECLUSION 22
1. BUSINESSES CANNOT ASSERT CLAIMS FOR INTRUSION UPON SECLUSION. 22
2. PLAINTIFFS FAIL TO ALLEGE MICROSOFT INTENTIONALLY INTRUDED UPON THEIR SECLUSION. 23

TABLE OF CONTENTS
(continued)

Page

3. PLAINTIFFS FAIL TO ALLEGE MICROSOFT'S PURPORTED INTRUSION WAS "HIGHLY OFFENSIVE." 24
4. PLAINTIFFS FAIL TO ALLEGE ANY COGNIZABLE HARM CAUSED BY THE PURPORTED INTRUSION. 25
IV. CONCLUSION 25

TABLE OF AUTHORITIES

Page

Cases

Backhaut v. Apple Inc.,
723 F. App'x 405 (9th Cir. 2018) 10

Bass v. Facebook, Inc.,
394 F. Supp. 3d 1024 (N.D. Cal. 2019) 22

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007) 12, 13, 19

Blough v. Shea Homes, Inc.,
No. 2:12-CV-01493 RSM, 2014 WL 3694231 (W.D. Wash. July 23, 2014) 21

Brinkley v. Monterey Fin. Servs., LLC,
340 F. Supp. 3d 1036 (S.D. Cal. 2018) 17

Brinkley v. Monterey Fin. Servs., LLC,
No. 16-cv-1103-WQH-WVG, 2019 WL 4295327 (S.D. Cal. May 6, 2019) 17

Buckley v. Santander Consumer USA, Inc.,
No. C17-5813 BHS, 2018 WL 1532671 (W.D. Wash. Mar. 29, 2018) ..... *passim*

Burton v. Lehman,
103 P.3d 1230 (Wash. 2005) 16

Cahen v. Toyota Motor Corp.,
717 F. App'x 720 (9th Cir. 2017) 22

Campbell v. Facebook Inc.,
77 F. Supp. 3d 836 (N.D. Cal. 2014) 12, 14

Converse v. Vizio, Inc.,
No. C17-5897 BHS, 2020 WL 729804 (W.D. Wash. Feb. 13, 2020) 21, 22

Cousineau v. Microsoft Corp.,
992 F. Supp. 2d 1116 (W.D. Wash. 2012) 9, 10

Eclectic Props. E., LLC v. Marcus & Millichap Co.,
751 F.3d 990 (9th Cir. 2014) 19

FCC v. AT&T Inc.,
562 U.S. 397 (2011) 23

TABLE OF AUTHORITIES (continued)

Page

Fidelity Mortg. Corp. v. Seattle Times Co.,
213 F.R.D. 573 (W.D. Wash. 2003) 18

Fisher v. State ex rel. Dep't of Health,
106 P.3d 836 (Wash. Ct. App. 2005) 23, 24

Folgelstrom v. Lamps Plus,
195 Cal. App. 4th 986 (2011) 25

Gonzales v. Uber Techs., Inc.,
305 F. Supp. 3d 1078 (N.D. Cal. 2018) 10

In re Google Assistant Privacy Litig.,
No. 19-cv-04286-BLF, 2020 WL 2219022 (N.D. Cal. May 6, 2020) 7, 16

In re Google Inc. Gmail Litig.,
No. 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013) 12, 13, 14

In re Google Privacy Policy Litig.,
2013 WL 6248499 (N.D. Cal. Dec. 3, 2013) 12

In re Google, Inc. Privacy Policy Litig.,
No. C 12-01382 PSG, 2012 WL 6738343 (N.D. Cal. Dec. 28, 2012) 11

Gragg v. Orange Cab Co.,
942 F. Supp. 2d 1111 (W.D. Wash. 2013) 18

Hall v. EarthLink Network, Inc.,
396 F.3d 500 (2d Cir. 2005) 11

Heeger v. Facebook, Inc.,
No. 18-cv-06399-JD, 2019 WL 7282477 (N.D. Cal. Dec. 27, 2019) 10

Huong Hoang v. Amazon.com, Inc.,
No. C11-1709MJP, 2012 WL 1088165 (W.D. Wash. Mar. 30, 2012) 22

Indoor Billboard/Wash., Inc. v. Integra Telecom of Wash., Inc.,
170 P.3d 10 (Wash. 2007) 19

Intercity Maint. Co. v. Local 254 Serv. Emps. Int'l Union,
62 F. Supp. 2d 483 (D.R.I. 1999) 23

In re iPhone Application Litig.,
844 F. Supp. 2d 1040 (N.D. Cal. 2012) 24

Keodalah v. Allstate Ins. Co.,
449 P.3d 1040 (Wash. 2019) 18, 21

TABLE OF AUTHORITIES (continued)

Page

Konop v. Hawaiian Airlines, Inc.,
302 F.3d 868 (9th Cir. 2002) 11, 12

Life Designs Ranch, Inc. v. Sommer,
364 P.3d 129 (Wash. Ct. App. 2015) 23

Maple v. Costco Wholesale Corp.,
No. CV-12-5166-RMP, 2013 WL 5885389 (E.D. Wash. Nov. 1, 2013) 20

Mark v. King Broad. Co.,
618 P.2d 512 (Wash. Ct. App. 1980), *aff'd sub nom. Mark v. Seattle Times*, 635 P.2d 1081 (Wash. 1981) 24

Minnick v. Clearwire US, LLC,
683 F. Supp. 2d 1179 (W.D. Wash. 2010) 21

Nemykina v. Old Navy, LLC,
No. 2:19-cv-01958 BJR, --- F. Supp. 3d ---, 2020 WL 2512884 (W.D. Wash. May 15, 2020) 18

Poore-Rando v. United States,
C16-5094 BHS, 2017 WL 5756871 (W.D. Wash. Nov. 28, 2017) 23

Quon v Arch Wireless Operating Co.,
529 F.3d 892 (9th Cir. 2008) 15

Reid v. Pierce Cty.,
961 P.2d 333 (Wash. 1998) 23

Rosenow v. Facebook, Inc.,
No. 19-cv-1297-WQH-MDD, 2020 WL 1984062 (S.D. Cal. Apr. 27, 2020) 12

State v. Fowler,
139 P.3d 342 (Wash. 2006) 17

State v. Smith,
540 P.2d 424 (Wash. 1975) 9

Svenson v. Google Inc.,
65 F. Supp. 3d 717 (N.D. Cal. 2014) 10

Theofel v. Farey-Jones,
359 F.3d 1066 (9th Cir. 2004) 11

Vess v. Ciba-Geigy Corp. USA,
317 F.3d 1097 (9th Cir. 2003) 19

TABLE OF AUTHORITIES (continued)

Page

Warth v. Seldin
422 U.S. 490 (1975) 7

Water & Sanitation Health, Inc. v. Rainforest All., Inc.,
No. C15-75RAJ, 2015 WL 12657110 (W.D. Wash. Dec. 29, 2015) 18, 19, 20

Weidenhamer v. Expedia Inc.,
No. C14-1239RAJ, 2015 WL 7157282 (W.D. Wash. Nov. 13, 2015)....21

Woodell v. Expedia Inc.,
No. C19-0051JLR, 2019 WL 3287896 (W.D. Wash. July 22, 2019)....20

Yunker v. Pandora Media, Inc.,
No. 11-CV-03113 JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013)....25

In re Zynga Privacy Litig.,
750 F.3d 1098 (9th Cir. 2014) 9

Statutes

18 U.S.C.
§ 2510(4)....9
§ 2510(5)(a)(ii)....12
§ 2511....2
§ 2511(1)(a) 9
§ 2520(a) 6
§ 2701....16
§ 2701(a) 16
§ 2701(c)(1) 16
§ 2702....2, 15
§ 2702(a)(1) 9, 15
§ 2702(a)(2) 9
§ 2702(b)(5) 14, 15
§ 2707(a) 6
§ 2711(2)....15
§ 2510(15) 11, 15
§ 2510(17) 15

Wash. Rev. Code
Ann. § 9.73.010....2
Ann. § 9.73.030....17
Wash. Rev. Code Ann.
§ 9.73.030(1)(a) 9, 16
§ 9.73.060....6, 16, 17
Ann. § 19.86....2

TABLE OF AUTHORITIES (continued)

Page

§19.86.....7
§ 19.86.090.....6

Other Authorities

Electronic Communications Privacy Act of 1986,
S. Rep. No. 99–541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555 12

Fed. R. Civ. P.
Rule 8 13
Rule 9 19
Rule 9(b) 18, 19, 20
Rule 12(b)(6).....1, 2, 16, 17

Restatement (Second) of Torts
§ 652B (1977) 23
§ 652I 23

NOTICE OF MOTION AND MOTION TO DISMISS

PLEASE TAKE NOTICE that on December 1, 2020, at 2:00 p.m. or as soon thereafter as this motion may be heard before the Honorable Judge Yvonne Gonzalez Rogers in Courtroom 1 of the United States District Court for the Northern District of California, 1301 Clay Street, Oakland, California, 4th Floor, Defendant Microsoft Corporation ("Microsoft") will move pursuant to Federal Rule of Civil Procedure 12(b)(6) to dismiss the Complaint (ECF No. 1) on the basis that it fails to state claims on which relief may be granted. This Motion is based on this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, the Request for Judicial Notice and related exhibits filed herewith, all pleadings on file in this matter, and other matters as may be presented to the Court.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiffs Frank D. Russo (sole proprietor of Russo Mediation & Law), Koonan Litigation Consulting, LLC, and Davenport & Associates, LLC, are three Microsoft customers who used Microsoft 365 software (previously known as Office 365) in operating their businesses. They claim Microsoft improperly shared customer data with third parties, namely Facebook, application developers, and subcontractors. Plaintiffs' Complaint, however, is more notable for what it does *not* allege. Plaintiffs do not allege facts plausibly showing Microsoft used or shared any of *their* data, much less without consent. Nor do Plaintiffs allege they saw and relied upon any of the statements they now complain about when they purchased Microsoft 365 services and decided which features to use. Plaintiffs also do not deny they received the full benefit of the services they bought; in fact, it appears from the Complaint they continue to use them. Instead of alleging any such facts, Plaintiffs rely in their Complaint on sweeping statements untethered to their own experiences, and on mischaracterizations of the Microsoft services at issue.[1] Based on these allegations, Plaintiffs seek to

[1] The following article provides further context on this case and concludes: "[t]hese shocking allegations are accompanied by no evidence. None." https://www.zdnet.com/article/class-action-comedy-is-microsoft-stealing-its-business-customers-data/. This Motion does not depend on the conclusions in this article, but the Court may review it for general background.[2] Plaintiffs allege that Washington law applies based on choice-of-law provisions in certain contracts. Compl. ¶¶ 129-133.

bring claims on behalf of a nationwide class of "persons and non-governmental entities" for alleged violations of the Wiretap Act ("WTA"), 18 U.S.C. § 2511 *et seq.*, the Stored Communications Act ("SCA"), 18 U.S.C. § 2702 *et seq.*, the Washington Consumer Protection Act ("CPA"), Wash. Rev. Code 19.86 *et seq.*, and the Washington Privacy Act ("WPA"), Wash. Rev. Code 9.73.010 *et seq.*, and for intrusion upon seclusion under Washington law.[2] The Court should dismiss the Complaint under Rule 12(b)(6) with prejudice for the following reasons:

First, Plaintiffs plead no facts plausibly showing *they* were affected by the alleged unlawful practices. Plaintiffs may not base their claims on generalized grievances with Microsoft's practices, or on speculation about the alleged experiences of others. The Court should dismiss the Complaint on this basis, alone.

Second, Plaintiffs cannot assert claims under the WTA, SCA, or WPA because Plaintiffs do not allege facts establishing the essential elements of these claims. For instance, all three statutes limit claims to the alleged misuse of "communications" (and in the case of the WPA, only "private" communications). Yet Plaintiffs do not allege they ever used Microsoft 365 to send or receive any communications. Indeed, when stripped of its sensationalism, the Complaint boils down to nothing more than a series of allegations that Microsoft provided services to customers in the ordinary course of, and necessarily incident to, its business—conduct the WTA and SCA expressly exempts. What's more, the WPA does not apply extraterritorially or to business entities like Plaintiffs Koonan and Davenport. For these and other reasons, the Court should dismiss the WTA, SCA, and WPA claims.

Third, Plaintiffs' CPA claim fails because Plaintiffs do not allege facts plausibly establishing causation or injury to Plaintiffs' business or property. Plaintiffs claim Microsoft misrepresented its data-related practices, but do not allege they ever saw those alleged misrepresentations, much less that those supposed misrepresentations influenced Plaintiffs' buying decisions. Plaintiffs also do not allege facts connecting the alleged misstatements to the price they paid for Microsoft 365 services, or that having their data placed "at risk" resulted in any tangible injury to their business or property.

Fourth, Plaintiffs do not allege essential elements of their claim for intrusion upon seclusion

[2] Plaintiffs allege that Washington law applies based on choice-of-law provisions in certain contracts. Compl. ¶¶ 129-133.

under Washington law. Plaintiffs, as businesses, cannot allege a violation of personal privacy interests. Moreover, Microsoft cannot have "intruded" as a matter of law because Plaintiffs voluntarily granted Microsoft access to their data by choosing to use its cloud-based services. Further, like the WTA and SCA, Washington's intrusion upon seclusion tort does not implicate practices performed in the ordinary course of business, such as those alleged here. Finally, Plaintiffs again do not allege that Microsoft's purported intrusion caused them any harm.

II. BACKGROUND

A. Microsoft 365 Services.

Microsoft offers a suite of well-known productivity applications and services for personal and business use, including Word, Outlook, Excel, PowerPoint, and Teams, among others. Microsoft 365 is the umbrella term for a variety of Microsoft offerings, which include different combinations of these software applications and services at different price points. Compl. ¶ 46. This case specifically involves the "Business" and "Enterprise" categories of Microsoft 365 services. *Id.* ¶ 116. Microsoft 365 customers span an immense range, from individuals to small business entities to the largest corporations in the world—all of which Plaintiffs have lumped together in their proposed class definition. *Id.*

B. Plaintiffs.

Plaintiff Russo "operates a sole proprietorship called Russo Mediation & Law," through which he provides "mediation, arbitration, and alternative dispute resolution services . . . ." *Id.* ¶ 13. Plaintiff Koonan is a California limited liability corporation that "provides its clients with advice on how to succeed in all aspects of litigation . . . ." *Id.* ¶ 21. Plaintiff Davenport is a Wyoming limited liability corporation that provides marketing services. *Id.* ¶ 28. Plaintiffs allege they have been "regular user[s] of Office 365 in the course" of their businesses since 2015 (Russo) and 2016 (Koonan and Davenport). *Id.* ¶¶ 15, 23, 34. Plaintiffs chose different Microsoft 365 offerings, presumably based on the specific applications and features they wanted. For example, Plaintiffs Russo and Davenport used Microsoft 365 Business Standard, *id.* ¶¶ 14, 29-31, while Plaintiff Koonan chose Microsoft 365 Business Basic, *id.* ¶ 22, which does not include Outlook as a desktop application, *see* Declaration of Whitty Somvichian ("Somvichian Decl.") Ex. C. Plaintiffs do not deny they received the services they

selected and paid for under their respective plans. Nor do they allege they have stopped using Microsoft 365, despite filing this lawsuit.

C. Plaintiffs' Allegations.

Plaintiffs' Complaint involves four primary theories of alleged improper use and disclosure of Microsoft 365 users' data.

First, Plaintiffs allege Microsoft "shares its business customer's contacts with Facebook" through a "Facebook-sharing 'feature'" in "Office 365 or Exchange Online services . . . ." *Id.* ¶¶ 75-76. Although Plaintiffs try to obscure the context, documents quoted in the Complaint (without attribution) explain this feature was previously an integrated part of Outlook known as "Facebook Contact Sync," which allowed users to share "information in your Outlook Contacts folder with Facebook, and imports your Facebook friends' contact information into your Outlook Contacts folder." *See* Somvichian Decl. Ex. A at 6. Plaintiffs admit Microsoft informed them they could "disable[] this Facebook-sharing 'feature'" but Plaintiffs do not say whether they did so. Compl. ¶ 76.

Second, Plaintiffs contend Microsoft "shares its business customers' data with third-party developers, so they can develop and sell new services and products . . . ." *Id.* ¶ 81. Plaintiffs omit any meaningful context for this allegation, but a document they quote (again without attribution) shows this allegation relates to Microsoft Graph, a platform that allows third-party developers to "build smarter apps" that integrate with Microsoft 365. *See* Somvichian Decl. Ex. B. Plaintiffs' selective quotation of the document omits the part explaining that Microsoft 365 "users' data is carefully managed, protected, and ***with proper authorization***, made available by Microsoft Graph services to drive productivity and creativity in businesses." *Id.* at 1 (emphasis added). In another notable omission, Plaintiffs quote a portion of the document that states third-party developers can "perform searches for people who are relevant to the [Microsoft] user and have expressed an interest in communicating with that user," Compl. ¶ 84, but omit the portion that explains developers can do so only if "***your app has got permissions by that user***." *Id.* at 3 (emphasis added).

Plaintiffs' theory of disclosures to third-party developers seems to relate to a hypothetical scenario in which two Microsoft 365 users exchange information and *one* of them has installed a third-

party application that uses the data to provide added functionality to that user's Microsoft 365 system. Compl. ¶¶ 81-83. Plaintiffs allege that in this situation the data for the *other* user that did *not* install the application (labeled by Plaintiffs as the "non-consenting business customers") can be transmitted to the third-party developer to enable the application, without consent from the "non-consenting" user. *Id.* Plaintiffs effectively concede, however, that the Microsoft 365 user who installed the application necessarily consented to the third-party developer's use of data. *See id*. ¶ 82 (alleging a business customer "did not consent to sharing its data with the third-party" if it "did *not* download a third-party application") (emphasis added).

Third, Plaintiffs claim Microsoft shares business customers' data with subcontractors. Plaintiffs do not allege there is anything improper *per se* with Microsoft engaging subcontractors to help provide services to users, but they speculate that in some instances, Microsoft does so to "serve Microsoft's separate commercial ventures, including discovering new business insights and developing new services, products, or features for Microsoft's benefit . . . ." *Id.* ¶ 87.

Fourth, and relatedly, Plaintiffs allege Microsoft "uses its business customers' data to develop and sell new products and services that benefit only Microsoft." *Id.* ¶ 91. As examples, the Complaint identifies various security-related services, including "Windows Defender Application Control, Azure Advanced Threat Protection, and Advanced Threat Protection" programs—all applications and services designed to *protect* users from cyberattacks and other threats.[3] *Id.* ¶¶ 95, 96. For example, the Complaint's reference to "Advanced Threat Protection" appears to refer to Office 365 Advanced Threat Protection, which "safeguards [enterprise customers'] organization[s] against malicious threats posed by email messages, links (URLs), and collaboration tools." Somvichian Decl. Ex. F. Advanced Threat Protection is part of certain Microsoft 365 offerings, depending on the options the customer selects. *Id*. Plaintiffs can hardly claim Microsoft somehow acted improperly by providing services that *protect* Plaintiffs and their data.

[3] Azure Advanced Threat Protection is a cloud-based security solution that helps Azure users detect threats to their own security networks. *See* Somvichian Decl. Ex. D. Windows Defender Application Control is a free feature included in Windows 10 (Microsoft's current Windows operating system) that allows system administrators to limit what programs users on a network can use to prevent malware and other malicious intrusions. Somvichian Decl. Ex. E.

In addition to these theories, Plaintiffs argue Microsoft and its subcontractors employ inadequate data security measures. Compl. ¶¶ 100-113. For example, Plaintiffs allege Microsoft fails to comply with data security standards known as SOC 1 and SOC 2. *Id.* ¶¶ 104, 108. But this theory depends on selectively quoting and mischaracterizing Microsoft's public statements. Regardless, Plaintiffs allege no facts to show *they* were affected by any alleged data security deficiencies.

Last, Plaintiffs allege throughout the Complaint that Microsoft intentionally misrepresents to Microsoft 365 customers the extent to which, and the circumstances under which, it uses business customers' data or shares such data with third parties. *Id.* ¶¶ 2-8, 45-113, 177-185. Plaintiffs, however, do not allege they ever reviewed, much less relied upon, any of the allegedly misleading statements identified in the Complaint in deciding which services to buy and use.

D. The Alleged Causes of Action & Proposed Class.

Based on these allegations, Plaintiffs assert claims for violations of the WTA, the SCA, the Washington CPA, and the WPA; they also allege a claim for intrusion upon seclusion under Washington common law. Plaintiffs seek to represent a nationwide class of "[a]ll persons and non-governmental entities in the United States who subscribed to or purchased" a variety of services they allege are related to Microsoft 365, from July 17, 2016 to the present. *Id.* ¶ 116.

III. ARGUMENT

A. Plaintiffs Fail to Allege Facts Plausibly Showing They Were Affected by Any of the Alleged Conduct.

As a fundamental matter, Plaintiffs cannot state a claim by merely asserting generalized complaints about Microsoft's alleged privacy practices; they must state sufficient facts to show these practices were actually applied to them individually. For instance, the WTA only provides a civil action to a "person whose . . . electronic communication is intercepted." 18 U.S.C. § 2520(a). That means Plaintiffs cannot base a WTA claim on alleged interceptions involving others. Similarly, the SCA only permits a civil action for persons "aggrieved by any violation[,]" so Plaintiffs cannot rely on alleged violations that did not affect them personally. 18 U.S.C. § 2707(a). Plaintiffs' other causes of action also require them to show they were individually impacted by the alleged practices. *See* Wash. Rev. Code Ann. § 9.73.060 (limiting civil actions to claimants who can show a violation of the

act "injured his or her business, his or her person, or his or her reputation"); Wash. Rev. Code Ann. § 19.86.090 (limiting civil action to "[a]ny person who is injured in his or her business or property by a violation of" Wash. Rev. Code Ann. §19.86 *et seq.*); *Buckley v. Santander Consumer USA, Inc.,* No. C17-5813 BHS, 2018 WL 1532671, at *7 (W.D. Wash. Mar. 29, 2018) (intrusion upon seclusion requires a plaintiff to plead "[a]n intentional intrusion, physically or otherwise, upon the solitude or seclusion of plaintiff, or his private affairs").

Plaintiffs cannot circumvent this basic requirement by resorting to the class action device. Even in a class action, the named plaintiffs "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." *Warth v. Seldin*, 422 U.S. 490, 502 (1975); *See also In re Google Assistant Privacy Litig*., No. 19-cv-04286-BLF, 2020 WL 2219022, at *7 (N.D. Cal. May 6, 2020) (granting motion to dismiss class action complaint where the allegations did "not suffice to show that Plaintiffs' own oral communications were intercepted").

Here, Plaintiffs fail to allege any facts plausibly showing they were individually affected by the practices of which they complain. They allege only that they are "regular user[s] of Office 365 in the course of" their businesses. Compl. ¶¶ 15, 23, 34. Apart from that conclusory statement, Plaintiffs allege no facts about which specific Microsoft 365 applications or features they used, how they used them, or any other facts plausibly showing the practices alleged in the Complaint ever applied to them. Each of Plaintiffs' theories of improper use/disclosure suffers from this fatal defect.

Regarding the Outlook feature that previously enabled synching contacts with Facebook, Plaintiffs do not allege they used Outlook at all, let alone that this specific Facebook feature was enabled[4] in their systems or configured to permit the data exchange as alleged.[5] *See id.* ¶¶ 74-77.

Similarly, Plaintiffs' third-party developer theory involves a specific circumstance that

[4] The article Plaintiffs quote at Paragraph 76 states "this feature *may be* turned on by default"; Plaintiffs notably do not allege it was in fact turned on by default in their systems. *See* Somvichian Decl. Ex. A at 7 (emphasis added).

[5] As described in the article Plaintiffs quote, the feature enabled synching of Outlook with "your Facebook friends' contact information," which necessarily required users to identify their Facebook account for the feature to work. *See* Somvichian Decl. Ex. A at 6.

Plaintiffs do not allege ever applied to them. Plaintiffs do not allege any one of them ever shared data with another Microsoft 365 user who installed a third-party application that Plaintiffs did not also use—*i.e.*, the "non-consenting business customer" hypothetical that is the premise of this theory. *Id.* ¶¶ 81-83. In fact, Plaintiffs do not allege they ever used Microsoft 365 to communicate with another Microsoft 365 user in *any* context.

Likewise, Plaintiffs' subcontractor theory does not rest on any facts regarding their own data. For example, they conclude—without any factual basis—that disclosing data to subcontractors exposes business customers to "a security and privacy risk." *Id.* ¶ 90. But Plaintiffs do not allege their data was actually provided to any subcontractors in the first instance. And even if they had so alleged, Plaintiffs concede several data security protections would have applied and offer no reason why these would not be adequate. *See id.* ¶¶ 88, 89 (referring to anonymization of "social security numbers [and] credit card numbers" and encryption of "credit card and bank account numbers, medical record numbers or biometric identifiers, and government-issued identification data").

Finally, Plaintiffs do not allege their data was actually used by Microsoft to develop "new products and services . . . ." *Id.* ¶ 91. Indeed, Plaintiffs do not even allege they used Microsoft 365 in a way that would have generated data that could be relevant to the services identified in the Complaint. *Id.* ¶ 87 (general allegations regarding using data for "artificial intelligence applications and development interfaces"); *id.* ¶¶ 93-96 (general allegations regarding using Microsoft 365 data to develop security applications and services including Windows Defender Application Control and others). Plaintiffs' concerns are thus entirely hypothetical.[6]

Fundamentally, the Complaint fails to allege facts plausibly showing Plaintiffs were impacted by the alleged practices. That Plaintiffs purport to bring this case as a class action makes no difference: Plaintiffs may not state a claim through generalized allegations and assumptions but rather must allege facts showing the practices about which they complain actually applied to them. They do not, and the Complaint should be dismissed in its entirety.

[6] Moreover, Plaintiffs consented in various ways to the use of their data to provide and improve Microsoft's services. Although beyond the scope of this Motion, this consent presents a dispositive defense to Plaintiffs' claims even if the claims could proceed past this Motion (and they should not).

B. The WTA, SCA, and WPA Claims Fail Because Plaintiffs Do Not Allege That The Alleged Practices Involved Their Communications.

Plaintiffs' WTA, SCA, and WPA claims fail for an independent reason: Plaintiffs do not allege facts showing Microsoft intercepted, disclosed, or recorded any of their communications. A plaintiff asserting a WTA and SCA claim must plead facts demonstrating the interception or disclosure of the "contents of . . . communication[s]" without consent. *See* 18 U.S.C. §§ 2702 (a)(1), (a)(2); *see also* 18 U.S.C. §§ 2510(4), 2511(1)(a). The contents of a communication must concern "the substance, purport, or meaning of [a] communication." *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) (citation omitted). This does not include record information, such as "the name, address, and subscriber number or identity of a subscriber or customer." *Id.* at 1106 (internal quotation marks and citation omitted).

The WPA is similar to the WTA and SCA but even narrower in scope, as it applies only to "[p]rivate" communications "transmitted . . . between two or more individuals . . . ." Wash. Rev. Code Ann. § 9.73.030(1)(a). Washington courts interpret "communication" under the WPA based on the "ordinary connotation of oral exchange, discourse, or discussion." *State v. Smith*, 540 P.2d 424, 428 (Wash. 1975). Transmitting data to a service provider is therefore not a "communication" covered by the statute. *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1129 (W.D. Wash. 2012) (granting motion to dismiss WPA claim because "[w]ithout an individual on the other end of her communication (other than Microsoft), the transmission of Cousineau's data cannot be considered a communication under the WPA").

Here, Plaintiffs do not state any facts showing Microsoft intercepted or disclosed the "contents of [their] communications" (as the WTA and SCA require), much less that any such communications were "private communications" (as the WPA requires). Indeed, Plaintiffs do not allege they *ever* used Microsoft 365 to send any emails or other communications. If anything, the few facts Plaintiffs do plead suggest they did *not* use Microsoft 365 in ways that could have implicated the WTA, SCA, or WPA. For instance, Plaintiff Davenport alleges it conducted "online research to identify the best solution for its document management, backup, and other business needs," with no reference to Outlook or any of Microsoft 365's *communications* features. Compl. ¶ 33. This would tend to show

that Plaintiff Davenport was not interested in, and did not use, Microsoft 365's communications features. For its part, Plaintiff Koonan alleges it subscribed to Microsoft 365 Business Basic, which does not include Outlook as a desktop application, suggesting it did not intend to use Microsoft 365 for business email communications. Regardless, the lack of any facts plausibly establishing that Microsoft misused any of Plaintiffs' communications mandates dismissing their WTA, SCA, and WPA claims. *See Heeger v. Facebook, Inc.*, No. 18-cv-06399-JD, 2019 WL 7282477, at *3 (N.D. Cal. Dec. 27, 2019) (granting motion to dismiss SCA claim because Plaintiff "does not allege that the 'contents' of a communication . . . were divulged"); *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1086-87 (N.D. Cal. 2018) (granting motion to dismiss WTA claim for failure to allege that content was intercepted).

Plaintiffs also may not support this claim through generalized allegations regarding the Facebook synch option, as that theory rests on the supposed sharing of data *other than* communications. Plaintiffs allege the data shared was "business customers' contacts . . . ." Compl. ¶ 75. Contact information, however, is not the "contents of a communication" under the WTA and SCA. *See Svenson v. Google Inc.*, 65 F. Supp. 3d 717, 728-30 (N.D. Cal. 2014) (granting motion to dismiss WTA claim where plaintiff's claim involved the disclosure of contact information). Nor is it a "private communication" within the meaning of the WPA. *See Cousineau*, 992 F. Supp. 2d at 1129 (WPA applies only where there is "an individual on the other end of her communication"). Plaintiffs therefore may not base a WTA, SCA, or WPA claim on this Facebook theory.

C. Plaintiffs' WTA Claim Fails For Additional Reasons.

Plaintiffs' WTA claim also fails because (1) Plaintiffs do not allege Microsoft intercepted any communications in "transmission," as required by the statute, and (2) any alleged interceptions fall within the "ordinary course of its business" exception to liability.

1. Plaintiffs Do Not Allege Microsoft Intercepted Any Communications In "Transmission."

To state a WTA claim, a plaintiff must allege facts showing the defendant intercepted the contents of a communication "during transmission, not while it is in electronic storage." *Backhaut v. Apple Inc.*, 723 F. App'x 405, 407 (9th Cir. 2018) (quoting *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d

868, 878-80 (9th Cir. 2002) (unauthorized access to communications stored on a secure website's bulletin board does not amount to an "interception")). The narrow scope of the WTA is "consistent with the ordinary meaning of 'intercept,' which is 'to stop, seize, or interrupt in progress or course before arrival.'" *Konop*, 302 F.3d at 878 (citation omitted); *see also Theofel v. Farey-Jones*, 359 F.3d 1066, 1077-78 (9th Cir. 2004) (no "acquisition contemporaneous with transmission" where the defendant accessed emails stored on an internet service provider's servers). Where a WTA claim is directed at the provider of an "electronic communications service" as defined in the WTA ("ECS"),[7] courts agree there is no interception where the ECS provider merely accesses communications of its users stored on its servers. *See In re Google, Inc. Privacy Policy Litig.*, No. C 12-01382 PSG, 2012 WL 6738343, at *6 (N.D. Cal. Dec. 28, 2012) (holding Google does not "intercept" user information on its servers and noting the lack of "any authority that supports … the notion that a provider can intercept information already in its possession"); *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 505 (2d Cir. 2005) (holding it would be an "absurd result" to find that an ECS provider intercepts the communications of its users because "their basic services involve the 'acquisition of the contents' of electronic communication." (citation omitted)).

Plaintiffs concede Microsoft 365 is an ECS and Microsoft is an ECS provider. Compl. ¶¶ 135, 137, 150. Plaintiff thus cannot state a WTA claim based on Microsoft's alleged access to Microsoft 365 customers' data stored on its servers. Yet that is the entire thrust of the Complaint. Plaintiffs allege Microsoft allegedly misuses data not while it is in "transmission" but rather only after the data has been received and stored on Microsoft's servers. *See, e.g.*, Compl. ¶ 157 ("Plaintiffs' and Class Members' electronic communications are maintained on Microsoft's servers on their behalf, as they are subscribers and customers of Microsoft's service."); *id.* ¶ 102 (alleging Microsoft applies inadequate data security to protect data it received and "stored"). Plaintiffs do not allege (nor could they) that any unauthorized act occurred in the virtually instantaneous moments when communications are transmitted over wires or other media, as would be needed to demonstrate an interception in "transmission." *See Konop*, 302 F.3d at 878-79 & n.6 ("transmission time" of electronic

[7] 18 U.S.C. § 2510(15) defines an "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications."

communications "is very short because [an electronic communication] travels across the wires at the speed of light").

Plaintiffs may not save their claim by repeatedly incanting the term "interception," as a "formulaic recitation of the elements of a cause of action will not do . . . ." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007); *see also Rosenow v. Facebook, Inc.*, No. 19-cv-1297-WQH-MDD, 2020 WL 1984062, at *7-8 (S.D. Cal. Apr. 27, 2020) (granting motion to dismiss WTA claim where Plaintiffs' allegations of an interception were "conclusory"). Because Plaintiffs do not allege Microsoft intercepted their communications in transmission, the Court should dismiss the WTA claim.

2. The "Ordinary Course Of Its Business" ("OCB") Exception Bars Plaintiffs' Claim.

The WTA also exempts from liability any alleged interception that involves an ECS provider's own devices used "in the ordinary course of its business . . . ." 18 U.S.C. § 2510(5)(a)(ii). The purpose of the ordinary course of business exception is to help "the efficient operation of the communications system." *See Electronic Communications Privacy Act of* 1986, S. Rep. No. 99–541, at 37 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3591. Some courts have interpreted this exception as requiring some nexus between the alleged interception and the defendant's business as an ECS provider. *See In re Google Inc. Gmail Litig*. ("*Gmail*"), No. 13-MD-02430-LHK, 2013 WL 5423918, at *11 (N.D. Cal. Sept. 26, 2013) (OCB exception applies "where the interception facilitated or was incidental to provision of the electronic communication service at issue"); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 844 (N.D. Cal. 2014) (OCB exception applies to practices that are "related or connected to an electronic communication provider's service, even if it does not actually facilitate the service"). Other courts have held the OCB exception applies broadly so long as the practice serves a "legitimate business purposes." *In re Google Privacy Policy Litig.*, 2013 WL 6248499, at *11 (N.D. Cal. Dec. 3, 2013).

Microsoft's alleged conduct falls within the OCB exception under any of these formulations. By Plaintiffs' own characterization, the "electronic communication service" at issue is "Office 365 or Exchange Online," Compl. ¶ 137, which they allege is an integrated "suite of software products," *id*. ¶ 46. The OCB exception thus applies to any alleged "interception" that "facilitates," is "incidental

to," or is "related or connected to," the overall set of services and features that comprise Microsoft 365. Plaintiffs' theories of improper data use/disclosure all fall within this framework.

First, Plaintiffs concede that synching contacts with Facebook was a "feature" of Outlook, which is part Microsoft 365. Compl. ¶ 76. This alleged "interception" not only "facilitated" the ECS, it was *part of* the ECS as Plaintiffs define it, and is therefore plainly covered by the OCB exception.

Second, Plaintiffs' theory regarding third-party developers involves disclosures through the Microsoft Graph platform, which enables development of applications to extend the functionality of Microsoft 365 for the benefit of Microsoft's customers. Compl. ¶ 84; Somvichian Decl. Ex. B (describing Microsoft Graph platform). This also falls squarely within the OCB exception.

Third, to support their subcontractor-disclosure theory, Plaintiffs allege Microsoft disclosed enterprise customers' data to develop "new services, products, or features," not just "to provide customers with the services they purchased . . . ." Compl. ¶ 87. But Plaintiffs do not identify any specific "new services, products, or features," and there is no basis to conclude any theoretical disclosure to any subcontractor related to some function beyond Microsoft's business as an ECS provider. Plaintiffs' vague references to facilitating "artificial intelligence and development interfaces" fall short of stating a plausible claim, as those allegations say nothing about *Plaintiffs'* data or experiences, and regardless, could just as well relate to Microsoft 365-related features. *Twombly*, 550 U.S. at 556-57 (allegations that are consistent with wrongful conduct but "could just as well be" legitimate conduct do not satisfy Rule 8).

Fourth, Plaintiffs allege Microsoft used Microsoft 365 data to develop certain data security applications and services[8] and to improve Cortana (Microsoft's voice assistant), and they complain these features are not "necessary to provide Office 365 services." Compl. ¶¶ 96-98. But "necessity" is not the standard for determining when the OCB exception applies; what matters is whether the activity "facilitates" or is "incidental" to the normal operation of Microsoft's business as an ECS. *Gmail*, 2013 WL 5423918, at *7-8. Plaintiffs cannot seriously claim security applications and services do not satisfy this test. In fact, Plaintiffs concede these applications and services are intended for the

[8] Basic background on these security applications and services is set forth in Somvichian Decl. Exs. D-G.

benefit of Microsoft customers. *See* Compl. ¶¶ 92, 96 (alleging enterprise customers' data is used to provide "products" and "applications" for "customers").[9]

Moreover, Cortana and Advanced Threat Protection are *parts of* Microsoft 365, so any use of data to develop or improve these services would necessarily fall within the OCB exception. *See* Compl. ¶ 97 (describing how Office 365 users are prompted to configure Cortana when installing Officer 365); Somvichian Decl. Ex. G (describing integration of Cortana and Microsoft 365); Somvichian Decl. Ex. F (describing integration of Advanced Threat Protection as part of Microsoft 365). Plaintiffs complain that not all customers use Cortana, Compl. ¶ 97, but that is immaterial. The relevant question for applying the OCB exception is whether the "interception" has the requisite relationship to the ECS provider's business—not whether a plaintiff happens to use a specific feature offered by the provider. *Gmail*, 2013 WL 5423918, at *11 (applying OCB exception hinges on whether the alleged interception facilitates the service).[10]

In short, the alleged "interceptions" here all fall within the OCB exception because they involve Microsoft's use of data in the ordinary course of its business of providing Microsoft 365 and related services. For this independent reason, the Court should dismiss Plaintiffs' WTA claim.

D. Plaintiffs' SCA Claim Fails For Additional Reasons.

The Court should also dismiss Plaintiffs' SCA claim because the "necessarily incident" exception bars it, and the SCA does not apply to Microsoft's own use of data.

1. The "Necessarily Incident" Exception Bars Plaintiffs' Claim.

Under the SCA, providers of an ECS or a "remote computing service" are not liable for disclosures that are "necessarily incident to *the rendition of the service* . . . ." 18 U.S.C. § 2702(b)(5)

---

[9] This distinguishes the circumstances here from other cases in which some courts declined to apply the OCB exception. In *In re Google Inc. Gmail Litigation* and *Campbell*, the courts declined to find the alleged interceptions, which enabled targeted advertising, were covered by the OCB exception. *Gmail*, 2013 WL 5423918, at *7; *Campbell*, 77 F. Supp. 3d at 844. The courts in those cases rested their conclusion on the concern that targeted advertising primarily benefits the advertiser, not the ECS-provider's customer. Here, in contrast, the alleged uses of data are all for the benefit of Microsoft users, as Plaintiffs' own allegations confirm.

[10] Plaintiffs also refer to Microsoft's Audience Network, which does relate to advertising. Compl. ¶ 95. But Plaintiffs do not allege that Audience Network uses enterprise customers' *communications*, so this advertising tool does not implicate the SCA, WTA, or WPA.

(emphasis added). An ECS is a service that enables users "to send or receive wire or electronic communications[.]" 18 U.S.C. § 2510(15). A "remote computing service" ("RCS") is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18. U.S.C. § 2711(2). The term "computer … processing" encompasses a wide range of services used by "businesses of all sizes." *See Quon v Arch Wireless Operating Co.*, 529 F.3d 892, 901 (9th Cir. 2008) (quoting legislative history of the SCA explaining "businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services").

Plaintiffs allege Microsoft is both an ECS and RCS provider. Compl. ¶¶ 137, 152. The "necessarily incident" exception thus applies broadly to Microsoft's rendition of services in providing "electronic communication[s,]" data "storage," and "computer . . . processing"—the services encompassed by Microsoft's function as both an ECS and RCS provider. *See* 18 U.S.C. § 2702(b)(5); *id.* § 2510(15) & (17); *id.* § 2711(2).

Plaintiffs' own allegations show the alleged practices here were all "necessarily incidental" to this broad scope of services. Plaintiffs do not deny, and indeed reference documents in the Complaint showing, that the alleged disclosure of enterprise customer data either enabled features of Microsoft's existing services or helped it develop new ones for the benefit of Microsoft's customers. *See, e.g.*, Compl. ¶ 76 & Somvichian Decl. Ex. A at 6-7 (alleged disclosures to Facebook enabled a feature of Outlook); Compl. ¶ 84 & Somvichian Decl. Ex. B (alleged disclosures to third-party developers enabled applications that enhance the functionality of Microsoft 365); Compl. ¶ 96 & Somvichian Decl. Exs. D-G (use of data to develop security applications and services to *protect* customers' data). Plaintiffs do not identify any Microsoft service that would fall outside the broad categories of "electronic communication[s,]" "storage," or "computer . . . processing." *See* 18 U.S.C. § 2510(15) & (17); *id.* § 2711(2). Because the alleged disclosures of enterprise customers' data enabled Microsoft's services as an ECS and RCS provider, these supposed disclosures fall squarely within the § 2702(b)(5) exemption and cannot supply the basis for an SCA claim.

2. The SCA Claim Does Not Apply to Microsoft's Own Use Of Data.

Section 2702 of the SCA applies only where an ECS provider "knowingly divulge[s]" its users' communications to third parties. 18 U.S.C. §§ 2702(a)(1)-(3) (imposing liability on covered entities

that "knowingly divulge" information). Separately, Section 2701 of the SCA expressly permits an ECS provider to access data for its own use. *See* 18 U.S.C. § 2701(c)(1) (liability for unauthorized access does not apply to "the person or entity providing a wire or electronic communications service"). Applying these provisions, courts have routinely dismissed SCA claims where no disclosures to third-parties were at issue, and the claims were based on an ECS provider's access to and use of data stored on its own servers. *See, e.g.*, *In re Google Assistant Privacy Litig.*, 2020 WL 2219022, at *12 (granting motion to dismiss SCA claim and holding "Defendants' own use of Plaintiffs' data for advertising purposes does not constitute an unlawful 'disclosure.'").

So too, here. Plaintiffs seek to impose SCA liability on Microsoft for its own access to and use of customers data. *See* Compl. ¶¶ 91-99 (alleging Microsoft uses its business customers' data, without alleging an intentional disclosure to third parties). The SCA expressly permits this alleged conduct. The Court should therefore dismiss any SCA claim based on Microsoft's own alleged use of Plaintiffs' data.

E. The Washington Privacy Act Claim Fails For Multiple Additional Reasons.

Plaintiffs Koonan and Davenport cannot assert a claim under the WPA because they are not natural persons but rather LLCs. The WPA applies to a "[p]rivate communication … between two or more *individuals* . . . ." Wash. Rev. Code Ann. § 9.73.030(1)(a) (emphasis added). Reinforcing this limitation, the WPA's civil remedy applies only to "person[s.]" Wash. Rev. Code Ann. § 9.73.060 (providing civil remedy to "persons" who have been injured in "his or her" business, person, or reputation). The statute does not define "person[s,]" but the Court may turn to the ordinary meaning of persons, which is limited to natural persons.[11] *See Burton v. Lehman*, 103 P.3d 1230, 1234 (Wash. 2005), as corrected (Oct. 24, 2005) (noting in the context of construing a Washington statute that "[i]f the undefined statutory term is not technical, the court may refer to the dictionary to establish the meaning of the word"). The Court should apply this common-sense interpretation and dismiss the WPA claims of Plaintiffs Koonan and Davenport because they are both LLCs.

Even if that were otherwise, the WPA claim would still fail as to all Plaintiffs for the additional

[11] *Person*, *Meriam-Webster.com*, https://www.merriam-webster.com/dictionary/person (last visited Sept. 23, 2020).

reason that Plaintiffs do not allege any interception occurred in Washington. As the Washington Supreme Court has explained, the WPA has no extraterritorial reach and thus, does not apply to recordings that occur outside of Washington. *State v. Fowler*, 139 P.3d 342, 347 (Wash. 2006) (finding WPA did not apply to call recorded in Oregon and holding "the test for whether a recording of a conversation or communication is lawful is determined under the laws of the place of the recording"). Here, the Complaint lacks any facts showing any interception occurred in Washington. That is fatal to Plaintiffs' WPA claim. *See Brinkley v. Monterey Fin. Servs., LLC*, No. 16-cv-1103-WQH-WVG, 2019 WL 4295327, at *3 (S.D. Cal. May 6, 2019) (dismissing WPA claim under Rule 12(b)(6) because "the complaint fails to allege any recordings which were made in Washington in violation of [Wash. Rev. Code] § 9.73.030").

Plaintiffs' WPA claim fails for yet another reason. To obtain civil recovery under the WPA, a person must be "injured" by the alleged violation. Wash. Rev. Code Ann. § 9.73.060. A violation of the statute alone does not suffice to show injury. *See Brinkley v. Monterey Fin. Servs., LLC*, 340 F. Supp. 3d 1036, 1045 n.3 (S.D. Cal. 2018) (dismissing WPA claim under Rule 12(b)(6) because the plaintiff failed to sufficiently allege she had been "injured"). Plaintiffs allege no facts showing they suffered any injury from any purported interception of their communications, which further requires dismissing this claim.[12]

F. Plaintiffs Fail to State a Claim Under the Washington Consumer Protection Act.

To state a CPA claim, Plaintiffs must allege facts establishing "(1) an unfair or deceptive act or practice that (2) affects trade or commerce and (3) impacts the public interest, and (4) [that Plaintiffs] sustained damage to business or property that was (5) caused by the unfair or deceptive act or practice." *Keodalah v. Allstate Ins. Co.*, 449 P.3d 1040, 1047 (Wash. 2019) (affirming dismissal of CPA claim). Failure to plead any one of these elements is fatal to a CPA claim. *Id.* As Plaintiffs allege Microsoft violated the CPA through intentionally deceptive conduct, Plaintiffs must plead those

[12] Plaintiffs allege they "paid for Microsoft's services" in an apparent effort to suggest an injury to support their WPA claim. Compl. ¶ 175. But an injury must be caused by "a violation of this statute" to support a civil remedy under the WPA. Wash. Rev. Code Ann. § 9.73.060. Plaintiffs' payments to Microsoft have nothing to do with any alleged interception and thus are not an "injury" that can support a viable WPA claim.

elements under Fed. R. Civ. P. 9(b)'s heightened pleading standard.[13] Plaintiffs do not sufficiently allege causation or injury to their business or property, requiring dismissing their CPA claim.

1. The CPA Claim is Subject to Rule 9(b)'s Heightened Pleading Standard.

The heightened pleading standard in Rule 9(b) applies when a plaintiff's CPA claim "mirrors the elements of an action for fraud." *Fidelity Mortg. Corp. v. Seattle Times Co.*, 213 F.R.D. 573, 575 (W.D. Wash. 2003) (finding CPA claim premised on allegation that publication "knowingly publish[ed] false, deceptive, and/or misleading information" must satisfy Rule 9(b) pleading standard (alteration in original)). Rule 9(b) applies to CPA claims based on a course of conduct that is essentially fraudulent in character, even if the plaintiff does not expressly mention "fraud" in the complaint. *Nemykina v. Old Navy, LLC*, No. 2:19-cv-01958 BJR, --- F. Supp. 3d ---, 2020 WL 2512884, at *2 (W.D. Wash. May 15, 2020) (finding CPA claim based on allegedly deceptive marketing subject to Rule 9(b) because it alleged a "unified course of fraudulent conduct" (citation omitted)); *Water & Sanitation Health, Inc. v. Rainforest All., Inc.*, No. C15-75RAJ, 2015 WL 12657110, at *3 (W.D. Wash. Dec. 29, 2015) (applying Rule 9(b) where defendant was alleged to have intentionally misled consumers by certifying noncompliant farms).

Rule 9(b) applies to Plaintiffs' CPA claim here because Plaintiffs accuse Microsoft of essentially fraudulent conduct. The central theory of their CPA claim is Microsoft intentionally misrepresented its privacy practices by saying it would not share customers' data with certain entities or use customers' data for certain purposes despite knowing it would do so. *See* Compl. ¶¶ 2-8, 45-113, 185. Plaintiffs further argue Microsoft knew privacy was material to its customers and made the alleged misrepresentations to induce customers' purchases. *Id.* ¶¶ 2-3, 47-53, 100-113, 185. For example, Plaintiffs allege Microsoft "knows that business customers would not share their data" with providers that do not comply with SOC Standards, promises customers it complies with SOC

[13] Plaintiffs do not allege a per se CPA violation and none of the statutes on which they rely (the WTA, SCA, and WPA) makes a violation a per se CPA violation. Thus, even if Plaintiffs were seeking to rest their CPA claim on supposed violations of those statutes, they would still need to establish each of the five elements of their CPA claim. *See, e.g.*, *Gragg v. Orange Cab Co.*, 942 F. Supp. 2d 1111, 1117 (W.D. Wash. 2013) (plaintiff pleading violation of Commercial Electronic Mail Act must separately plead injury and causation to state a CPA claim).

standards, and encourages customers to rely on these promises, all while knowing it collects customer data in Graph, a tool Microsoft allegedly knows is not SOC-compliant. *Id.* ¶¶ 100-113. Plaintiffs also conclude Microsoft "abused [its] position in order to exploit its customers' data," and "Microsoft's deception was deliberately orchestrated to conceal its intrusions from Plaintiffs and Class Members." *Id.* ¶¶ 166(f), 185. Allegations like these that a defendant made false statements and "knew about the falsity of its representations" describe a fraudulent course of conduct and, as such, are subject to Rule 9(b). *See Water & Sanitation Health*, 2015 WL 12657110, at *3 (Rule 9(b) applies where plaintiff alleged "Defendant knew about the falsity of its representations . . . and nevertheless continued to issue certifications with the understanding that consumers would pay a price premium for its partners").

Consequently, in addition to alleging a plausible claim for relief, Plaintiffs must plead the circumstances giving rise to their CPA claim with particularity. *See Eclectic Props. E., LLC v. Marcus & Millichap Co.*, 751 F.3d 990, 995 & n.5 (9th Cir. 2014) ("[T]he plausibility analysis of *Twombly* and *Iqbal* applies equally to Rule 9 . . . ."). That is, Plaintiffs must plead "'the who, what, when, where, and how' of the misconduct charged." *Water & Sanitation Health*, 2015 WL 12657110, at *3 (quoting *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003)). Plaintiffs do not. They do not specify whether, much less when, they viewed, heard, read, or otherwise observed Microsoft's purportedly deceptive marketing and which marketing, or how that marketing, allegedly caused them to purchase Microsoft's services.

2. Plaintiffs Fail to Allege Microsoft's Purported Misconduct Caused Their Injuries.

To plead causation under the CPA, Plaintiffs must allege facts sufficient to show that "but for [Microsoft's] unfair or deceptive practice, [Plaintiffs] would not have suffered an injury." *Indoor Billboard/Wash., Inc. v. Integra Telecom of Wash., Inc.*, 170 P.3d 10, 22 (Wash. 2007). Where, as here, Plaintiffs base their CPA claim on allegedly deceptive marketing, they cannot plead causation unless they allege facts describing, with particularity, their review of the allegedly deceptive statements and how those statements caused Plaintiffs' alleged harm. *See Water & Sanitation Health*, 2015 WL 12657110, at *3 (dismissing CPA claim for failure to satisfy Rule 9(b) where plaintiff failed

to allege when it viewed the advertisements and purchased the offending products). Plaintiffs fail to plead such allegations with the requisite particularity under Rule 9(b); indeed, their Complaint lacks factual allegations showing causation entirely.

Plaintiffs' assertions of harm all relate to their decisions to purchase Microsoft services. Specifically, Plaintiffs allege that but for the challenged misrepresentations, they either would not have purchased the services or would have paid less for them. Compl. ¶ 114. But the Complaint is devoid of any facts connecting the alleged deceptive statements to the Plaintiffs, much less to their specific purchasing decisions. Plaintiffs do not allege which, if any, of the alleged deceptive statements they read. Instead, each Plaintiff makes the identical allegation that he/it "believed" Microsoft would keep data safe and secure, *id.* ¶¶ 17, 25, 36, without alleging which statements or information that plaintiff reviewed to form the basis of his/its belief. Likewise, each Plaintiff alleges Microsoft misrepresented material facts about the use and protection of data, *id.* ¶¶ 18, 26, 37, without alleging which purported misrepresentations were made to, or seen by, any individual plaintiff. Without such facts, Plaintiffs cannot establish the "but for" relationship between Microsoft's alleged conduct and their alleged harm necessary to plead causation.

Courts routinely dismiss CPA claims for similar pleading deficiencies. For example, in *Maple v. Costco Wholesale Corp.*, the court dismissed a complaint on causation grounds where the plaintiff failed to allege he had read the specific statements on a product label he claimed were misleading. No. CV-12-5166-RMP, 2013 WL 5885389, at *5 (E.D. Wash. Nov. 1, 2013). The court emphasized "broad conclusory statements on causation . . . could not overcome Plaintiff's failure to factually plead that he read the allegedly deceptive labels prior to purchasing the drink." *Id.* Similarly, in *Woodell v. Expedia Inc.*, the court dismissed a complaint for failure to allege causation because the plaintiff did not allege a deceptive "Taxes & Fees" charge affected her purchase decision. No. C19-0051JLR, 2019 WL 3287896, at *11-12 (W.D. Wash. July 22, 2019); *see also Minnick v. Clearwire US, LLC*, 683 F. Supp. 2d 1179, 1188 (W.D. Wash. 2010) ("None of the Plaintiffs identify the relied-upon statements and, therefore, they have not alleged a plausible basis to identify CPA causation.").

Plaintiffs' attempt to pursue their claims as a class action does not change the pleading standard. To the contrary, courts considering CPA claims stress the need for every allegedly aggrieved

party—both the named plaintiffs and absent class members—to prove he or she reviewed the alleged misstatements *and* those misstatements caused that individual party harm. For example, in *Weidenhamer v. Expedia Inc.*, the court observed "[c]ustomers who never saw the advertisements could not have relied upon any alleged misrepresentations contained therein . . . ." No. C14-1239RAJ, 2015 WL 7157282, at *12 (W.D. Wash. Nov. 13, 2015); *see also Converse v. Vizio, Inc.*, No. C17-5897 BHS, 2020 WL 729804, at *10 (W.D. Wash. Feb. 13, 2020) (causation requires showing the allegedly injured party viewed the alleged representation and had his or her purchasing decision influenced by it); *Blough v. Shea Homes, Inc.*, No. 2:12-CV-01493 RSM, 2014 WL 3694231, at *12 (W.D. Wash. July 23, 2014) (causation requires showing of whether purchases were predominantly based on the misrepresentation, and whether and to what extent class members knew about defects concealed by the misrepresentation). Plaintiffs' failure to allege causation here dooms their CPA claim.

3. Plaintiffs Do Not Adequately Allege CPA Injury.

A plaintiff asserting a CPA claim must allege injury to business or property. *Keodalah*, 449 P.3d at 1047. Plaintiffs have not done so. They assert two forms of supposed injury: first, "they paid more for a service or product advertised as having certain qualities . . . when in fact the product did not have those qualities," Compl. ¶ 167(b), and second, Microsoft's data sharing practices placed Plaintiffs' data "at risk," *id.* ¶ 167(c). But Plaintiffs do not adequately plead either.

As to the first theory of injury, Plaintiffs do not allege facts plausibly connecting Microsoft's representations about data privacy to the value of the service they purchased. Each Plaintiff allegedly subscribed to versions of Microsoft 365, a cloud-based service providing access to Microsoft Office features such as Word, Outlook, Excel, and PowerPoint, paying either $12.50 per month, $119.88 per year, or $150 per year. *Id.* ¶¶ 14, 22, 29-33, 46. Plaintiffs admit these features offer myriad functions, ranging from communication, scheduling, word processing, presentations, and many more. *Id.* ¶¶ 33, 46; *see also* Somvichian Decl. Ex. B. And Plaintiffs do not deny they received the services for which they paid. Given Plaintiffs acknowledge their purchases gave them access to an extensive suite of features, applications and services, the amount they paid for those services is equally (if not more so) consistent with the value those services provided as it is with Plaintiffs' (speculative) theory. That is,

Plaintiffs have not alleged facts plausibly showing they paid more than the services were worth, even assuming the representations were false. *See Cahen v. Toyota Motor Corp.*, 717 F. App'x 720, 723 (9th Cir. 2017) (affirming dismissal of deceptive marketing claims for lack of injury based on overpayment for vehicles because plaintiffs failed to allege facts supporting conclusion that vehicles were worth less due to alleged defects); *cf. Converse*, 2020 WL 729804, at *10 (a "bare assertion [of price inflation] is insufficient" to prove injury).

As to the second theory of injury, an enhanced risk of disclosure is not recognized as a cognizable injury under the CPA. Indeed, consumer protection claims premised on the misuse of data must allege more concrete harm than simply placing data "at risk." *See, e.g.*, *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1040 (N.D. Cal. 2019) (finding allegations of future risk and loss of time in connection with data breach insufficient to establish injury elements of claims under California's Unfair Competition Law and Consumers Legal Remedies Act). CPA claims based on the release of information can only proceed when there are allegations of discrete harm caused by that release. *See, e.g.*, *Huong Hoang v. Amazon.com, Inc.*, No. C11-1709MJP, 2012 WL 1088165, at *1, *6 (W.D. Wash. Mar. 30, 2012) (disclosure of actress's age allegedly harmed her by lowering her chances of being cast to play younger women); *Buckley*, 2018 WL 1532671, at *3 (disclosure of plaintiff's personal information led to plaintiff being targeted in a fraudulent debt collection scheme). Plaintiffs have not identified any discrete harm resulting from Microsoft's alleged use or sharing of their data. Plaintiffs, therefore, have not adequately pled the injury element of their CPA claim.

G. Plaintiffs Fail to State a Claim for Intrusion Upon Seclusion.

Plaintiffs' claim for intrusion upon seclusion under Washington law fails because businesses may not invoke the tort and Plaintiffs do not allege Microsoft intentionally intruded upon their seclusion, such intrusion was "highly offensive," or they suffered any injury as a result of the purported intrusion, each of which is a required element of this claim. *Buckley*, 2018 WL 1532671, at *7 (dismissing intrusion upon seclusion claim).

1. Businesses Cannot Assert Claims for Intrusion Upon Seclusion.

Washington's tort of intrusion upon seclusion is a common law cause of action allowing individuals to vindicate their privacy rights. *Fisher v. State ex rel. Dep't of Health*, 106 P.3d 836, 840

(Wash. Ct. App. 2005); *see also* Restatement (Second) of Torts § 652B (1977). This right is a personal one, available only to the individual whose privacy is invaded. *See* Restatement (Second) of Torts § 652I; *Reid v. Pierce Cty.*, 961 P.2d 333, 339 (Wash. 1998) (adopting Restatement definition of right to privacy). Companies do not enjoy privacy rights under Washington law; thus, they cannot bring intrusion upon seclusion claims. *See, e.g.*, *Life Designs Ranch, Inc. v. Sommer*, 364 P.3d 129, 139 (Wash. Ct. App. 2015) (["[A] corporation has no personal right of privacy and thus has no cause of action for invasion of privacy."); *accord FCC v. AT&T Inc.*, 562 U.S. 397, 406-07 (2011) ("personal privacy" does not apply to corporate entities); *Intercity Maint. Co. v. Local 254 Serv. Emps. Int'l Union*, 62 F. Supp. 2d 483, 506 (D.R.I. 1999) (under Restatement, "a corporation does not enjoy privacy rights").

Each plaintiff here seeks relief for alleged intrusion upon business, not personal, privacy. Two plaintiffs—Koonan and Davenport—are companies and therefore barred from asserting an intrusion claim. And while Russo, the remaining plaintiff, purports to sue in his individual capacity, his claims exclusively relate to the operation of his (sole proprietor) business and Microsoft's alleged use of his business data. Compl. ¶¶ 13-16. Washington's intrusion upon seclusion tort does not allow Russo to sue for alleged intrusion on his business's information.

2. Plaintiffs Fail to Allege Microsoft Intentionally Intruded Upon Their Seclusion.

To plead an intrusion upon seclusion claim, a plaintiff must allege the defendant "believes, or is substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act." *Buckley*, 2018 WL 1532671, at *7 (quoting *Poore-Rando v. United States*, C16-5094 BHS, 2017 WL 5756871, at *2 (W.D. Wash. Nov. 28, 2017)). A defendant cannot commit an intentional intrusion when the plaintiff has voluntarily provided the information in question to the defendant. That is precisely what Plaintiffs allege here. They voluntarily purchased and used Microsoft's services, providing their data to Microsoft in the process. Compl. ¶¶ 14-15, 22-23, 29-32, 34. Microsoft's access to Plaintiffs' data thus resulted from Plaintiffs' own acts, not any intentional intrusion on Microsoft's part.

Buckley v. Santander Consumer USA, Inc. is illustrative. The plaintiff in *Buckley* financed a

car purchase through the defendant, providing her personal information to the defendant in the process. After she defaulted on her debt, the defendant provided her information to a debt collector, which Buckley alleged was an intrusion upon her seclusion. 2018 WL 1532671, at *1, *7. But the *Buckley* court found the defendant had permission to access the plaintiff's information because she provided it to the defendant in connection with the loan financing, thus defeating any claim for intentional intrusion. *Id.* at *7.

The logic of *Buckley* applies here with equal force. Plaintiffs granted Microsoft access to their data by using its services, thereby precluding claims Microsoft intentionally intruded upon their private affairs. And to the extent Plaintiffs' claims rest on Microsoft's alleged data-sharing practices, those claims cannot be construed as ones for intrusion. *Id*. Nor can they survive as claims for disclosure because Plaintiffs do not plead disclosure to the public at large. *See Fisher*, 106 P.3d at 840-41.

3. Plaintiffs Fail to Allege Microsoft's Purported Intrusion Was "Highly Offensive."

An intrusion upon seclusion "is actionable only if the interference with a plaintiff's seclusion is a substantial one resulting from conduct of a kind that would be highly offensive and objectionable to the ordinary person." *Mark v. King Broad. Co.*, 618 P.2d 512, 519 (Wash. Ct. App. 1980), *aff'd sub nom. Mark v. Seattle Times*, 635 P.2d 1081 (Wash. 1981). As a matter of law, Microsoft's alleged privacy practices, performed in the ordinary course of its business, are not "highly offensive," and therefore are not implicated by the tort Plaintiffs assert.

Courts routinely reject intrusion and other privacy claims where the practices at issue involved normal business activities. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (dismissing claim because collection of personal information from consumers' phones was routine commercial behavior, not a "serious invasion" of privacy); *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980, at *14(N.D. Cal. Mar. 26, 2013) (similar); *Folgelstrom v. Lamps Plus*, 195 Cal. App. 4th 986, 992 (2011) (obtaining plaintiff's address and using it to mail advertisements is "not an egregious breach of social norms, but routine commercial behavior" (citation omitted)). The same reasoning dictates that Microsoft's alleged practice of acquiring data with

Plaintiffs' permission in the normal course of its business is not "highly offensive."

4. Plaintiffs Fail to Allege Any Cognizable Harm Caused by the Purported Intrusion.

Plaintiffs do not allege facts showing they suffered damage caused by the alleged misconduct. *See Buckley*, 2018 WL 1532671, at *7. Plaintiffs' allegation of injury is wholly conclusory: "Plaintiffs and Class Members have suffered extensive damages as a direct and proximate cause of Microsoft's intrusions into its private affairs." Compl. ¶ 186. They identify no harm they suffered by virtue of Microsoft's alleged access to and use of their data. Plaintiffs may not assert injury by alleging price inflation, as Microsoft's alleged intrusion *after* Plaintiffs purchased Microsoft's services cannot have induced those purchases. Plaintiffs' assertion that Microsoft's alleged data-sharing practices placed their data "at risk" likewise does not allege injury under this tort because those practices are not actionable via an intrusion claim. Plaintiffs' failure to allege facts suggesting that Microsoft's mere access to data caused them harm is fatal to their intrusion upon seclusion claim.

IV. CONCLUSION

Plaintiffs fail to state a viable cause of action because they do not adequately allege they have been impacted by the alleged practices and do not plead facts plausibly establishing essential elements of their claims. Accordingly, the Court should dismiss the Complaint in its entirety.

Dated: October 5, 2020

By: */s/ Michael Rhodes*
COOLEY LLP
Michael G. Rhodes (116127)
Whitty Somvichian (194463)
Priyamvada Arora (301207)
Colin S. Scott (318555)